CHARTA LEARNING · LESSON NOTES

Managing Outsourcing Risk

FRM Part II

1 A story: the outage that was not Kestrel's fault

- Kestrel hands card payments to Northgate
- A four-hour outage at Northgate on a busy Friday
- Customers, press and supervisor blame Kestrel
- The problem stays with the bank

IN THE LESSON

- Imagine that Kestrel Bank hands its card payment processing to Northgate, a specialist that promises to run it more cheaply and more reliably than Kestrel could.
- For two years all goes well.
- Then, on a busy Friday, Northgate's systems fail for four hours.
- Kestrel's customers cannot pay in shops, the complaints pour in, and the newspapers write about Kestrel, not Northgate.
- The next morning the supervisor phones Kestrel's chief executive and asks what the bank is doing about it.
- Kestrel's managers protest that the failure happened at Northgate.
- The supervisor's reply is the theme of this lesson.
- You chose the provider, you agreed the contract, and the customers are yours, so the problem is yours.

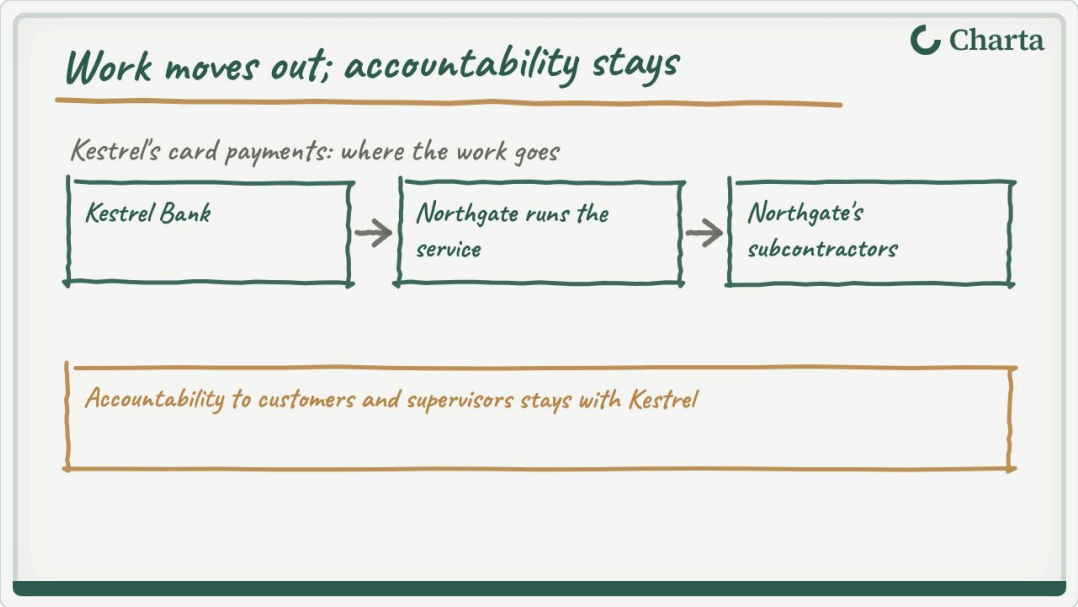
2 What outsourcing is

- Paying a third party for work the bank could do
- Examples: IT, payments, call centres, back office
- Why: cost, skills, scale, focus
- The bank keeps full responsibility
- The contract moves the work, not the accountability

IN THE LESSON

- Let us define the idea.
- Outsourcing means a bank pays a third party, called a service provider, to perform an activity the bank could perform itself.
- Typical examples are information technology, payment processing, call centres, and back office work such as account administration.
- Banks outsource for familiar reasons: lower cost, specialist skills, scale, and the freedom to focus on their core business.
- Those benefits are real.
- But one thing does not move with the work.
- The bank keeps full responsibility to its customers and to its supervisors for the outsourced activity, exactly as if it still did the work in house.
- The contract moves the work.
- It does not move the accountability.

3 Work moves out; accountability stays



IN THE LESSON

- Here is the picture to keep in mind.
- Follow the top row, where Kestrel's card payment work goes, from left to right.
- Kestrel Bank hands the work to Northgate, which runs the service day to day.
- Northgate in turn may hand parts of the work to its own subcontractors, for example a cloud company that hosts its servers.
- So the work can travel two or more steps away from the bank.
- Now look at the bottom row.
- Accountability to customers and to supervisors does not travel along that chain.
- It stays with Kestrel.
- When anything in the chain fails, the customer still holds an account at Kestrel, and the supervisor still regulates Kestrel.
- That is why the bank must manage the provider's risk as if it were its own.

4 Risks that outsourcing creates

The first group of risks

Risk	How outsourcing creates it
Operational	Failure at the provider
Compliance	Provider breaches laws or rules
Strategic	Misaligned with the bank's goals
Reputation	Customers blame the bank

IN THE LESSON

- So what can go wrong?
- The first group of risks is shown here.
- Operational risk is the risk of loss from failed processes, people or systems, and now those processes sit at the provider, where the bank cannot see them directly.
- The Friday outage is an example.
- Compliance risk is the risk that the provider breaks a law or rule on the bank's behalf, such as a data protection or consumer rule, and the bank answers for it.
- Strategic risk arises when the arrangement does not fit the bank's goals, or when the bank loses the skills to run or judge the activity itself.
- Reputation risk is the damage to the bank's name when the provider lets customers down.

5 More risks: credit, country, concentration

Three more risks to name in an exam

Risk	How outsourcing creates it
Credit, counterparty	The provider weakens or fails
Country	Services or data sit abroad
Concentration	Many functions on one provider

IN THE LESSON

- Three more risks complete the list.
- Credit or counterparty risk arises because the provider is itself a firm that can weaken or fail.
- If Northgate runs short of money, it may cut staff or investment, or stop the service entirely.
- Country risk arises when the services or the data sit abroad.
- Political events, foreign laws or a foreign court can then affect the service, and the bank's supervisor may find the data hard to reach.
- Concentration risk arises when many critical functions depend on one provider, or on a few providers that share the same infrastructure underneath, such as one cloud company.
- Then a single failure can stop several critical services at once.

6 Example 1: hidden concentration

Kestrel's five critical functions: who runs them, and on what?

Critical functions	at Kestrel Bank	**5**
Run by Northgate	payments, online, ledger	**3**
Other firm, same cloud	the call centre	**1**
Share on one cloud	(3 + 1) ÷ 5	**80%**
One failure stops	4 of 5 critical functions	**Concentration**

IN THE LESSON

- Let us measure Kestrel's concentration.
- Kestrel has five critical functions, meaning activities whose failure would seriously harm customers or the bank.
- Northgate runs three of them: card payments, online banking and the core ledger.
- A fourth, the call centre, is run by a different firm, so it looks diversified.
- But that firm hosts its systems on the same cloud company that Northgate uses.
- So four of the five critical functions rest on one shared infrastructure.
- Three plus one, divided by five, is eighty per cent.
- One failure at that cloud company could stop four of Kestrel's five critical functions together.
- The lesson is to look through the provider names to what lies underneath.

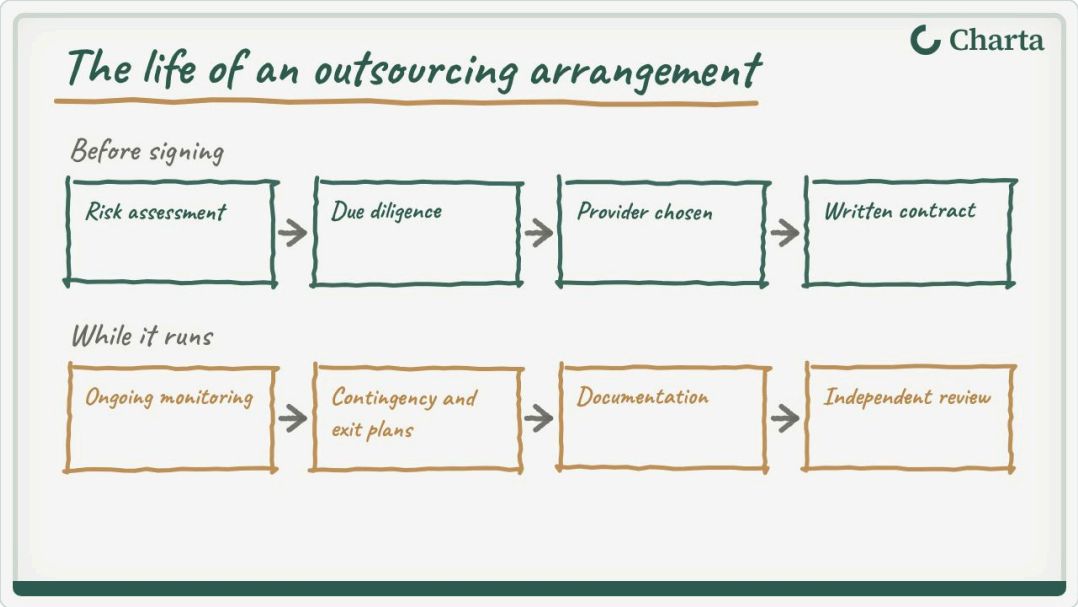
7 An effective outsourcing program

- Approved and overseen by the board
- Risk-based: effort follows risk
- Policies and procedures set by senior management
- Covers the whole life of each arrangement
- Oversight scales with criticality, not the fee

IN THE LESSON

- How does a bank control all this?
- With an outsourcing risk management program, and the exam asks for its features.
- First, the program is approved by the board of directors, which also oversees it.
- Second, it is risk based.
- The effort the bank spends on an arrangement depends on how much risk the arrangement carries.
- Third, senior management sets the policies and procedures that put the program into practice and makes sure there are people to run it.
- Fourth, the program covers the whole life of every arrangement, from the first idea to the exit.
- And the key principle is that the intensity of oversight scales with how critical the activity is, not with the size of the fee.

8 The life of an outsourcing arrangement



IN THE LESSON

- Here is that life, in the order the bank works through it.
- Before signing, the bank first runs a risk assessment before each decision to outsource: what could go wrong, and is outsourcing still worth it?
- Next comes due diligence on the candidate providers.
- Then the bank chooses the provider.
- Then a written contract fixes the terms, and the service begins.
- While it runs, the bank carries out ongoing monitoring of performance and of the provider itself.
- It keeps contingency and exit plans ready in case the provider fails or the relationship must end.
- It keeps documentation of every decision and review.
- And an independent review, for example by internal audit, checks that the whole program works.

9 Example 2: criticality, not the fee

Score 1 to 3 on impact, data, replaceability, regulation. 10 or more is critical

Canteen: annual fee	staff catering	**$2.0m**
Canteen: criticality score	1 + 1 + 1 + 1	**4 of 12**
Payments: annual fee	Northgate	**$0.8m**
Payments: criticality score	3 + 3 + 2 + 3	**11 of 12**
Most oversight goes to	criticality, not the fee	**Payments**

IN THE LESSON

- Kestrel tiers its providers with a simple scoring rule of its own.
- Each arrangement scores one to three on four factors: impact on customers, sensitivity of the data, how hard the provider is to replace, and regulatory importance.
- A total of ten or more out of twelve makes the arrangement critical.
- The staff canteen contract costs two million dollars a year, but it scores one on every factor, so four out of twelve.
- Payment processing costs only eight hundred thousand dollars a year, yet it scores three, three, two and three, which is eleven out of twelve.
- The canteen fee is two and a half times as large, but payments is the critical arrangement and gets the most oversight.

10 Who does what in the program

Each role sits inside the bank, not at the provider

Role	What it does
Board	Approves program, oversees it
Senior management	Sets policies, gives resources
Relationship owner	Manages it day to day
Independent review	Checks the program works

IN THE LESSON

- A program needs clear roles.
- The board approves the program, sets how much outsourcing risk the bank will accept, and receives reports on the critical arrangements.
- Senior management sets the policies and procedures and provides the people and resources to run them.
- A named relationship owner in the business manages each arrangement day to day, watching performance and raising problems.
- And an independent function, such as internal audit, reviews whether the program actually works as designed and reports to the board.
- Notice that none of these roles sits at the provider.
- Northgate can report to Kestrel, but it cannot take over any of Kestrel's responsibilities.

11 Exam trap: indemnities do not transfer the risk

- Claim: an indemnity or insurance transfers the risk
- Wrong: they repay some money, within limits
- They do not restore trust or reputation
- The supervisor still holds the bank to account
- They never replace managing the provider

IN THE LESSON

- Now the classic exam trap.
- Someone argues that the risk has been transferred because the contract makes the provider indemnify the bank, meaning repay its losses, or because the bank has insurance.
- That is wrong.
- An indemnity or an insurance policy can repay some money, but only up to its limits, only if the provider or insurer can and does pay, and only after a delay.
- It does not restore the customers' trust or the bank's name.
- It does not stop the supervisor holding the bank to account.
- So indemnities and insurance reduce the financial cost of some losses.
- They never move the responsibility, and they are never a substitute for managing the provider.

12 What due diligence is

- A structured check: can the provider deliver safely?
- Done before the provider is selected
- Repeated while the relationship runs
- Depth proportional to criticality
- Not a one-off exercise

IN THE LESSON

- We now turn to due diligence.
- Due diligence is the bank's structured assessment of whether a provider can deliver the service safely.
- It answers a simple question: can this firm do what it promises, for as long as we need it, without exposing us to risks we cannot accept?
- Three features matter for the exam.
- First, diligence is done before the bank selects a provider.
- Second, it is repeated while the relationship runs, because providers change.
- Third, its depth is proportional to the criticality of the activity.
- Kestrel will dig far deeper into Northgate, which runs payments, than into the canteen company.
- Diligence is not a one off exercise.

13 What diligence looks at: the firm

Can the firm do the job, and for how long?

Area	The question it answers
Background, reputation, strategy	Track record and commitment
Financial condition	Able to last the whole term?
Operations, internal controls	People, systems, controls
Security, data protection	Customer data kept safe?

IN THE LESSON

- What does the bank examine?
- The first group of areas is about the firm itself.
- Business background, reputation and strategy: how long the provider has operated, what its other clients say, and whether this service is central to its future or a sideline it may drop.
- Financial condition: whether it is strong enough to perform over the full term of the contract.
- Operational capacity and internal controls: whether it has the people, systems and controls to handle Kestrel's volumes.
- Information security and data protection: how it protects customer data from theft, misuse and loss.
- For a payments provider like Northgate, those last two areas are where most of the work goes.

14 What diligence looks at: resilience and law

Can it keep going, legally, through its own suppliers?

Area	The question it answers
Continuity, disaster recovery	Survives a disruption?
Legal, regulatory compliance	Follows the rules?
Insurance	Real cover in place?
Subcontractors	Who else, and overseen how?
Conflicts of interest	Competing loyalties?

IN THE LESSON

- The second group of areas is about resilience, law and the wider chain.
- Business continuity and disaster recovery: how the provider keeps running, and how fast it recovers, after a fire, a power cut or a cyber attack.
- Legal and regulatory compliance: whether it follows the laws that apply to the service, and has any record of breaches.
- Insurance: what cover it holds, and whether that cover is large enough to matter.
- Subcontractors: which other firms it uses, and how it oversees them, since their failures become the provider's failures.
- Conflicts of interest: for example, a provider that also serves a direct competitor, or that is owned by someone connected to the bank.

15 Example 3: can the bidder last the term?

Bidder Brightway: $6.0m cash, net cash outflow $0.5m a month, 5-year contract

Cash held	Brightway Systems	**$6.0m**
Net cash outflow	per month	**$0.5m**
Runway	6.0 ÷ 0.5	**12 months**
Contract term	5 × 12	**60 months**
Runway as share of term	12 ÷ 60	**20%**

IN THE LESSON

- Kestrel is comparing Northgate with a cheaper bidder, Brightway Systems, for a new five year contract.
- Brightway has six million dollars of cash.
- It is growing fast and losing money, so its cash falls by a net half a million dollars a month.
- Six million divided by half a million gives a runway of twelve months, meaning Brightway runs out of cash in a year unless it raises more.
- The contract term is five years, which is sixty months.
- Twelve over sixty is twenty per cent.
- So on its own resources Brightway can fund only a fifth of the term.
- That is a red flag.
- Kestrel needs more evidence, such as committed funding, before it can rely on Brightway.

16 Depth of diligence follows criticality

Kestrel's own rule: deeper and more often for critical arrangements

Tier	Depth	Repeated
Critical	Full, on site, tests	Every year, on change
Moderate	Standard questionnaire	Every 2 years
Low	Basic check	At renewal

IN THE LESSON

- Since diligence is proportional, Kestrel sets out how deep it goes for each tier, using its scoring rule from earlier.
- For a critical arrangement such as payments, diligence is full: on site visits, a review of financial statements, tests of security and continuity, and a look at the main subcontractors.
- It is repeated at least every year and whenever something important changes.
- For a moderate arrangement, Kestrel uses a standard questionnaire and the provider's documents, and repeats the work every two years.
- For a low risk arrangement such as the canteen, a basic check is enough, repeated when the contract is renewed.
- These are Kestrel's own choices, but the principle is general.

17 Independent audit reports: use them with care

- An outside auditor tests the provider's controls
- Useful input, never relied on blindly
- Check scope: does it cover what the bank uses?
- Check period: which months, and how long ago?
- Read the exceptions and the bank's own duties

IN THE LESSON

- A useful input to diligence is an independent audit report on the provider's controls.
- An outside auditor tests the provider's controls and reports the results, so many clients can rely on one piece of work.
- These reports save time, but the bank cannot rely on them blindly.
- It must check the scope: which services, systems and locations the report covers, and whether that includes what the bank actually uses.
- It must check the period: which months were tested, and how long ago that period ended.
- It should read the exceptions, meaning the controls that failed a test.
- And it should note any controls the report assumes the bank runs itself.

18 Example 4: reading Northgate's audit report

Report received in October. Does it cover what Kestrel relies on?

Period tested	January to June	**6 months**
Since the period ended	July to October	**4 months**
Data centres in scope	of Northgate's 3	**2**
Kestrel's data held in	the centre left out	**Not covered**
Exceptions reported	access controls	**1**

A useful input: Kestrel fills the gaps itself

IN THE LESSON

- In October, Kestrel receives Northgate's latest independent controls report.
- The report covers six months, January to June.
- By the end of October, four months have passed since the period ended, July to October, and nothing tells Kestrel how controls worked in those months.
- Next, scope.
- Northgate runs three data centres, but the report covers only two.
- Kestrel's data sits in the one that was left out, so for Kestrel's purposes the report covers nothing about where its data lives.
- Finally, the report lists one exception, in access controls.
- The report is still useful as an input, but Kestrel must fill the gaps itself, for example by asking about the missing months and by testing the third site.

19 Diligence while the relationship runs

- Repeated on a schedule set by criticality
- Triggers: new owner, financial weakness
- Triggers: incidents, missed service levels
- Triggers: new subcontractor, data abroad, more reliance
- Trap: diligence finished once the contract is signed

IN THE LESSON

- Diligence does not end when the contract is signed.
- The bank repeats it on a schedule, as in Kestrel's tiers, and also when something important changes.
- Typical triggers are a change of ownership at the provider, signs of financial weakness such as losses or a rating downgrade, a serious incident or a pattern of missed service levels, a new subcontractor, a move of data to another country, and much greater reliance by the bank on the service.
- Each trigger means looking again at the areas we covered.
- The exam trap is treating diligence as finished once the contract is signed.
- Providers change, and the bank's risk changes with them.

20 Mistakes to avoid in due diligence

Each mistake leaves the bank knowing less than it thinks

Mistake	Better practice
Trusting a famous name	Check the facts
Trusting an audit report blindly	Check scope, period, exceptions
Same light check for all	Depth follows criticality
Ignoring subcontractors	Look through to fourth parties

IN THE LESSON

- Here are four mistakes to avoid.
- Relying on a famous name: a big provider can still be wrong for this service, so the bank checks the facts.
- Relying blindly on an audit report: as we saw, the bank checks the scope, the period and the exceptions.
- Doing the same light check for every provider: depth must follow criticality, so payments get far more attention than the canteen.
- And ignoring the subcontractors: the provider's own suppliers, sometimes called fourth parties, can fail too, as the cloud company in our concentration example shows.
- Each of these mistakes leaves the bank believing it knows a provider better than it does.

21 The contract: the bank's main tool

- Main tool to control work the bank no longer does
- Written, so it is clear and enforceable
- Reviewed by legal counsel before signing
- Proportionate to the risk of the activity

IN THE LESSON

- Once Kestrel has chosen Northgate, the contract becomes its main tool.
- The bank no longer does the work, so it cannot control it directly.
- What it can control is what the provider has promised, what the bank is allowed to see, and what happens when things go wrong.
- Three requirements apply to the contract itself.
- It should be written, so that the terms are clear and can be enforced.
- It should be reviewed by legal counsel before signing.
- And it should be proportionate to the risk of the activity: a detailed contract for payments, a simpler one for the canteen.
- Let us go through the subjects it should cover.

22 Contract subjects: the service and oversight

What exactly is done, and how the bank can check it

Subject	What the clause fixes
Scope of services	Exactly what is done
Performance, service levels	Measurable, with consequences
Reporting, incidents	Regular reports, prompt notice
Audit and access rights	Bank, auditors, supervisors

IN THE LESSON

- The first group of subjects defines the service and the bank's right to oversee it.
- Scope of services: exactly what the provider will do, and what it will not, so that nothing falls into a gap.
- Performance standards and service levels: measurable targets, such as availability and processing times, with consequences, such as fee reductions, when they are missed.
- A target that cannot be measured cannot be enforced.
- Reporting and incident notification: regular performance reports, and prompt notice of any incident that affects the service or the bank's data.
- Audit and access rights: the right for the bank, its auditors and its supervisors to examine the provider's records and operations.

23 Contract subjects: law, data and continuity

Keeping customers, data and service safe

Subject	What the clause fixes
Compliance with laws	Provider follows the rules
Confidentiality, data security	Information protected
Data ownership, location	Bank owns it; where it sits
Continuity, disaster recovery	Tested plans and targets

IN THE LESSON

- The second group protects customers and data.
- Compliance with laws: the provider must follow the laws and rules that apply to the service, including those the bank itself is subject to.
- Confidentiality: the provider must keep the bank's and customers' information secret.
- Data security: the controls it must maintain to protect that information.
- Ownership and location of data: the data belongs to the bank, and the contract says where it may be stored and processed, which matters if it may go abroad.
- Business continuity and disaster recovery: the provider must keep and test plans to keep running, with recovery targets the bank can check.

24 Contract subjects: when things go wrong

Change, failure, and who pays

Subject	What the clause fixes
Subcontracting	Conditions, notice, approval
Default and termination	Exit, transition, data back
Indemnity, liability, insurance	Who pays, up to how much
Disputes, governing law	Key for foreign providers

IN THE LESSON

- The third group deals with change and failure.
- Subcontracting: whether the provider may pass work to others, on what conditions, and with notice to or approval by the bank.
- Default and termination: the events that let the bank end the contract, plus transition assistance to move the service elsewhere, and the return of the bank's data.
- Indemnification, liability limits and insurance: who pays for which losses, up to what amount, and what cover backs that up.
- Dispute resolution and governing law: how disagreements are settled and which country's law applies.
- These matter most for a foreign provider, where a dispute could otherwise end up in an unfamiliar court.

25 Turning a service level into minutes

Allowed downtime = (1 − target availability) × minutes in period

Target availability	Promised share of time up
Minutes in the period	Measurement window in minutes
Allowed downtime	Time down before a miss

IN THE LESSON

- Service levels are where contract numbers appear in exams.
- Take availability, the share of time a service is working.
- A target of ninety nine point nine per cent sounds close to perfect, so translate it into minutes.
- Allowed downtime equals one minus the target availability, times the minutes in the period.
- The target availability is the promised share of time the service is up.
- The minutes in the period come from the measurement window in the contract, often a month.
- And the allowed downtime is how long the service can be down before the provider has missed its target.
- The translation shows what a target really permits, and the window matters.

26 Example 5: the four-hour outage, in numbers

Target 99.9% availability over a 30-day month; monthly fee $150,000

Minutes in the month	30 × 24 × 60	**43,200**
Allowed downtime	0.1% × 43,200	**43.2 min**
Actual outage	4 hours: target missed	**240 min**
Service credit	10% × $150,000	**$15,000**
Kestrel's own cost	compensation, extra staff	**$2.4m**

The credit covers 0.6% of Kestrel's cost: a service level is not insurance

IN THE LESSON

- Back to the Friday outage.
- Northgate's contract promises ninety nine point nine per cent availability over a thirty day month.
- Thirty days times twenty four hours times sixty minutes is forty three thousand two hundred minutes.
- Point one per cent of that is forty three point two minutes of allowed downtime.
- The outage lasted four hours, far longer than allowed, so the target is missed.
- Four hours is two hundred and forty minutes.
- The contract gives Kestrel a service credit of ten per cent of the monthly fee of one hundred and fifty thousand dollars, which is fifteen thousand dollars.
- Kestrel's own cost of compensation and extra staff is two point four million dollars.
- The credit covers about six tenths of one per cent of that cost.
- A service level is not insurance.

27 Example 6: the liability cap

Data breach at Northgate. Liability capped at 12 months of fees

Monthly fee	Northgate	**$150,000**
Liability cap	12 × $150,000	**$1.8m**
Cost of the breach	Kestrel's estimate	**$7.5m**
Kestrel bears	7.5 − 1.8	**$5.7m**
Share Kestrel bears	5.7 ÷ 7.5	**76%**

IN THE LESSON

- Now suppose a worse event, a data breach at Northgate.
- Northgate's contract caps its liability at twelve months of fees.
- The monthly fee is one hundred and fifty thousand dollars, so the cap is twelve times one hundred and fifty thousand, which is one point eight million dollars.
- Kestrel estimates the total cost of the breach at seven point five million dollars, covering customer compensation, fines and remediation.
- The most Northgate pays is the cap.
- Kestrel bears the rest: seven point five minus one point eight is five point seven million dollars, which is seventy six per cent of the cost.
- The liability cap decides how much real consequence the provider bears.

28 The usual mistake: caps and force majeure

- Mistake: a very low liability cap
- Mistake: a force majeure clause written too widely
- Force majeure: events beyond a party's control
- Too wide, it excuses the provider's own failures
- Continuity duties must still apply

IN THE LESSON

- This leads to the usual mistake with contracts.
- The bank accepts a liability cap so low, or a force majeure clause so wide, that the provider bears little real consequence for failing.
- Force majeure means events beyond a party's control, such as a natural disaster or war, that excuse it from performing.
- Written too widely, it can excuse the provider's own failures, for example any systems failure or any failure by a subcontractor.
- Yet surviving such events is exactly what the continuity and disaster recovery clause is for.
- So the bank should resist a very low cap, and make sure force majeure never excuses the provider's own continuity obligations.

29 Example 7: fixing Northgate's draft contract

Legal counsel marks up the draft before Kestrel signs

Draft clause	Kestrel's fix
No supervisor access	Access for bank, auditors, supervisors
Cap: 3 months' fees ($450,000)	Negotiate a higher cap
Free subcontracting	Notice and approval
Exit only on insolvency	Wider rights, transition help
Silent on data	All data returned at exit

IN THE LESSON

- Let us put this together.
- Northgate sends Kestrel a draft contract for a new service, also priced at one hundred and fifty thousand dollars a month, and Kestrel's legal counsel marks it up.
- The draft has no access right for supervisors, so Kestrel adds audit and access rights for itself, its auditors and its supervisors.
- The draft caps liability at three months of fees, which is four hundred and fifty thousand dollars, so Kestrel negotiates a higher cap.
- The draft lets Northgate subcontract freely, so Kestrel requires notice and approval.
- The draft allows termination only if Northgate becomes insolvent, so Kestrel adds wider termination rights with transition assistance.
- And the draft is silent on data, so Kestrel adds return of all its data at exit.

30 Why it matters: the exit you hope never to use

- On the worst day, contract and plans are all it has
- Needed: right to leave, transition help, data back
- An exit plan written in advance
- Program, diligence and contract work together

IN THE LESSON

- Why do these clauses matter so much?
- Because on the worst day, the contract and the plans behind it are all the bank has.
- If Northgate fails, Kestrel needs the right to leave, help to move the service, and its data back in a usable form.
- It also needs an exit plan already written, naming an alternative provider or a way to bring the work back in house.
- Without these, Kestrel is locked in, however badly Northgate performs.
- That is how the three parts of this lesson connect.
- The program decides how much care each arrangement gets.
- Diligence chooses a provider that can deliver.
- And the contract keeps control after signing, right up to the exit.

31 Try three quick questions

1. 99.5% availability over a 30-day month. Allowed downtime?
   Answer: 0.5% × 43,200 = 216 minutes = 3.6 hours.
2. Fee $80,000 a month, cap 6 months' fees, loss $3m. Bank bears?
   Answer: Cap $480,000. Bank bears $2.52m.
3. Provider gets a new owner and a new subcontractor. Diligence done?
   Answer: No: both trigger fresh due diligence.

IN THE LESSON

- Now try three quick questions.
- Pause the video, think, then listen to the answers.
- Question one.
- A contract promises ninety nine point five per cent availability over a thirty day month.
- How much downtime is allowed before the target is missed?
- Point five per cent of forty three thousand two hundred minutes is two hundred and sixteen minutes, which is three point six hours.
- Question two.
- A provider's monthly fee is eighty thousand dollars, and its liability is capped at six months of fees.
- A failure costs the bank three million dollars.
- How much does the bank bear?
- The cap is four hundred and eighty thousand dollars, so the bank bears two point five two million dollars.
- Question three.
- A year after signing, a provider is bought by a new owner and adds a subcontractor.
- Is the bank's due diligence finished?
- No.
- Both are triggers, so the bank repeats its diligence.